



# Die Corona-Warn-App unter der Lupe

**FALK SIPPACH**

JUG Saxony Day Online 2021

Freitag, 01.10.2021



1

## Die Corona-Warn-App unter der Lupe



### Zusammenfassung

Leuchtturmprojekt, Kostengrab, Hoffnungsträger und wichtiger Baustein in der Pandemiebekämpfung - das deutsche Corona-Warn-App-System (kurz CWA) besteht nicht nur aus den recht prominenten iOS- und Android-Apps. Zur Umsetzung von Use Cases wie der persönlichen Risikoermittlung oder dem Melden von (positiven) Testergebnissen, gehört auch eine vierteilige Server-Lösung. Sie basiert auf einem zeitgemäßen Architekturstil und einem aktuellen Technologie-Stack. Und wurde unter hohem Zeitdruck federführend von SAP und Deutscher Telekom realisiert.

Das öffentliche Interesse an diesem Projekt ist hoch, die Transparenz bei der Entwicklung erfreulicherweise ebenfalls. Der Quellcode ist Open Source und auch die Dokumentation offen zugänglich. Wir diskutieren die prägenden architekturelevanten Anforderungen und die getroffenen Entscheidungen. Zum Abschluss bewerten wir die gewählten Lösungsansätze und arbeiten Stärken, Hindernisse und Kompromisse heraus.



2

## Falk Sippach

- Softwarearchitekt, Berater, Trainer bei embarc
- früher bei Orientation in Objects (OIO), Trivadis

### Schwerpunkte:

- Architekturberatung und -bewertung
- Cloud- und Java-Technologien



✉ fs@embarc.de

🐦 @sipsack

🔗 → [xing.to/fsi](https://www.xing.to/fsi)



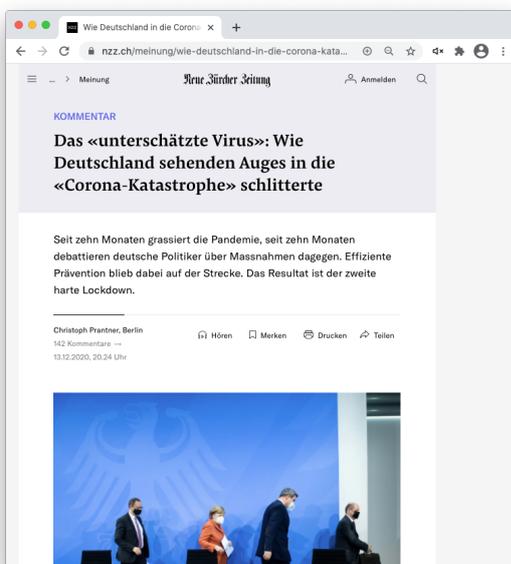
Falk Sippach: "CWA unter der Lupe"

embarc.de

3

3

## Neulich in den Medien ...



*“Die deutsche Corona-App ist womöglich unter Gesichtspunkten des Datenschutzes Weltklasse, für eine effiziente Bekämpfung der Pandemie allerdings so gut wie unbrauchbar.”*

Kommentar NZZ, 13.12.2020

Neue Zürcher Zeitung



Falk Sippach: "CWA unter der Lupe"

embarc.de

4

4

## Agenda



- 1 Einstieg und Motivation
- 2 Architekturelevante Anforderungen
- 3 Lösungsansätze
- 4 Stärken, Risiken und Kompromisse
- 5 Ausblick und weitere Informationen



5

## Agenda

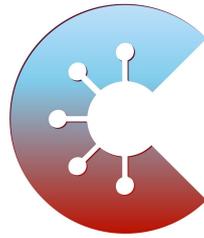


- 1 Einstieg und Motivation**
- 2 Architekturelevante Anforderungen
- 3 Lösungsansätze
- 4 Stärken, Risiken und Kompromisse
- 5 Ausblick und weitere Informationen

**1**



6



# Gemeinsam Corona bekämpfen

<https://www.coronawarn.app>



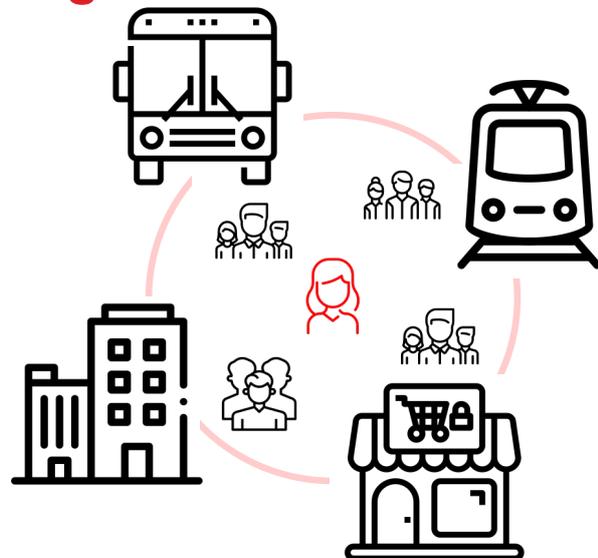
Falk Sippach: "CWA unter der Lupe"

embarc.de

7

7

## Warum ist die App so wichtig?



Falk Sippach: "CWA unter der Lupe"

embarc.de

8

8

## Wie funktioniert die App?



<https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-erklaerfilm-1758828>



Falk Sippach: "CWA unter der Lupe"

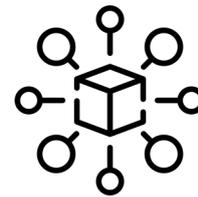
embarc.de

9

9

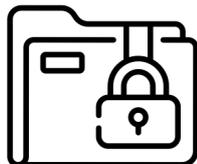
## Was passiert mit den Daten?

Keine  
Anmeldung



Dezentrale  
Speicherung

Keine  
Rückschlüsse  
auf persönliche  
Daten



Keine Einsicht  
für Dritte



Falk Sippach: "CWA unter der Lupe"

embarc.de

10

10



## Executive Summary



This document describes and analyzes a system for **secure and privacy-preserving proximity tracing at large scale**. This system provides a technological foundation to help **slow the spread of SARS-CoV-2** by simplifying and accelerating the process of notifying people who might have been exposed to the virus so that they can take appropriate measures to break its transmission chain. The system aims to **minimise privacy and security risks for individuals and communities and guarantee the highest level of data protection**.

### Decentralized Privacy-Preserving Proximity Tracing

Version: 25 May 2020.  
Contact the first author for the latest version.

**EPFL:** Prof. Carmela Troncoso, Prof. Mathias Payer, Prof. Jean-Pierre Hubaux, Prof. Marcel Salathé, Prof. James Larus, Prof. Edouard Bugnion, Dr. Wouter Lueks, Theresa Stadler, Dr. Apostolos Pyrgelis, Dr. Daniele Antonoli, Ludovic Barman, Sylvain Chatel

**ETHZ:** Prof. Kenneth Paterson, Prof. Srdjan Čapkun, Prof. David Basin, Dr. Jan Beutel, Dr. Dennis Jackson, Dr. Marc Roeschlin, Patrick Leu

**KU Leuven:** Prof. Bart Preneel, Prof. Nigel Smart, Dr. Aysajan Abidin

**TU Delft:** Prof. Seda Gürses

**University College London:** Dr. Michael Veale

**CISPA:** Prof. Cas Cremers, Prof. Michael Backes, Dr. Nils Ole Tippenhauer

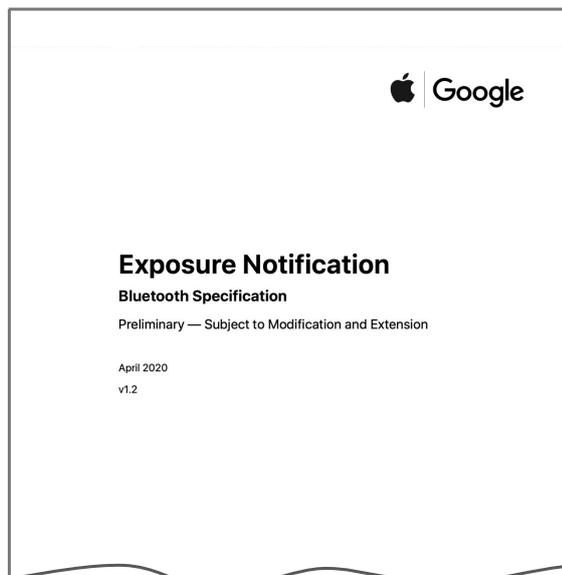
**University of Oxford:** Dr. Reuben Binns

**University of Torino / ISI Foundation:** Prof. Ciro Cattuto

**Aix Marseille Univ, Université de Toulon, CNRS, CPT:** Dr. Alain Barrat

**IMDEA Software Institute:** Prof. Dario Fiore

**INESC TEC:** Prof. Manuel Barbosa (FCUP), Prof. Rui Oliveira (UMinho), Prof. José Pereira (UMinho)



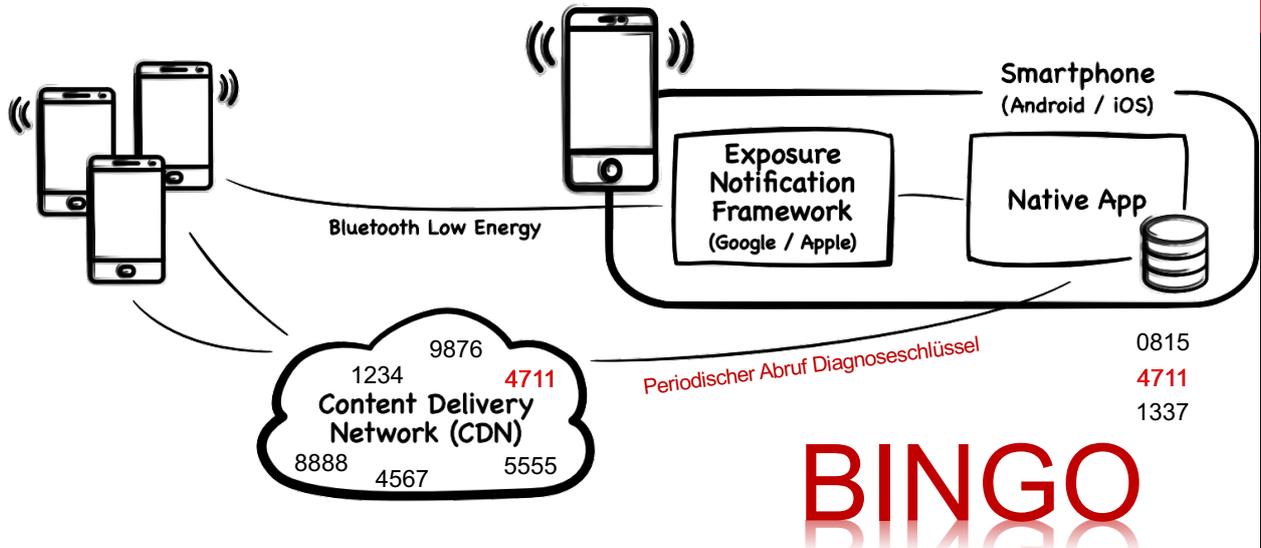
## Overview



This document provides the detailed technical **specification for a new privacy-preserving Bluetooth protocol** to support Exposure Notification. Exposure Notification makes it possible to combat the spread of the coronavirus — the pathogen that causes COVID-19 — by **alerting participants about possible exposure to someone they have recently been in contact with**, who has subsequently been positively diagnosed as having the virus. [...] uses the **Bluetooth Low Energy wireless technology for proximity detection of nearby smartphones**, and for the data exchange mechanism.



## Kontakt mit positiv Getesteten



# BINGO



Falk Sippach: "CWA unter der Lupe"

embarc.de

15

15

## Funktionsweise: Testen lassen

**Auftrag für SARS-CoV-2 Testung nach RVO oder regionaler Sondervereinbarung**  
 >>>>>>> Formular nicht kopieren! <<<<<<<<

**OGEG**

Name, Vorname des Geleisteten  
 Mustermann gen. von  
 Maxi  
 Musteradresse

geb. am 12.10.1982

Auftragsnummer des Labors  
 123456789

Abnahmedatum 19.08.2020

Abnahmesatz 1 | 0 | 0 | 8 | 2 | 0 | 1 | 0 | 3 | 5

RVO  
 § 4 Nr. 4 i) RVO Ausnahmefall  
 regionale Sondervereinbarung RV-Sonderfall

Erstentstehung  weitere Testung

§ 2 RVO Kontaktperson  § 3 RVO Ausnahmefall  
 § 2 RVO Miskung „erhöhtes Risiko“ durch Corona-Warn-App  § 4 Nr. 1-3 RVO Verhütung der Verbreitung  
 § 4 Nr. 4 i) RVO Risikogebiet (Inland)

Besondere Risikofaktoren einer Weiterverbreitung (z.B. berufliche, soziale, etc.)

Betreuung/Unterbringung in Einrichtung  Medizinischen Einrichtungen (z.B. Arztpraxis, Zahnarztpraxis, etc.)  Pflege- und anderen Wohnrichtungen (z.B. Altenheim, etc.)  
 Tätigkeit in Einrichtung  Gemeinschaftseinrichtungen (z.B. Kindertagesstätten, etc.)  Sonstigen Einrichtungen (z.B. Sportplatz, etc.)

**Freigabe 06.08.2020**

Einverständliche der Geleisteten zum Übermitteln der Testergebnisse für oder der Corona-Warn-App auf den vom RKI betriebenen Server wurde erteilt. Im Geleisteten wurden Hinweise zum Datenschutz ausgeblendet.  
 für das Gesundheitsamt - Übermittlung gemäß Infektionsschutzgesetz  
 Telefonnummer des Geleisteten

**Verbindliches Muster**

330008-3667F32-4DCF-43A5-8737-4CD1F81DF6DA

**Gemeinsam schnell die INFEKTIONSKETTE UNTERBRECHEN**  
 Die App als Beitrag, um die Pandemie weiter einzudämmen

Tragen Sie aktiv zur Eindämmung der Pandemie bei. Nutzen Sie die Corona-Warn-App. Die App zu nutzen ist ganz einfach. Ihre Daten sind dabei sicher und werden nicht weitergegeben.

- Laden Sie die App im Apple Store oder Google Play Store. Die App ist kostenlos.
- Richten Sie die App ganz einfach ein. Sie werden dabei in der App angeleitet.
- Scannen Sie den QR-Code und Sie erhalten eine Benachrichtigung, sobald Ihr Testergebnis vorliegt.
- Im Falle eines positiven Testergebnisses können Sie andere App-Nutzer freiwillig warnen.

**Hinweise zum Datenschutz:** Sie möchten die Corona-Warn-App (App) des Robert-Koch-Instituts (RKI) zum Abrufen Ihrer Testergebnisse verwenden. Um Ihr Testergebnis über die App abrufen zu können ist es notwendig, dass Ihr Testergebnis von dem Labor zu den Servern der App übermittelt wird. Hierzu benötigt die App Ihre Einwilligung. Bitte beachten Sie, dass die App keine personenbezogenen Daten speichert und keine Daten an Dritte weitergibt. Die App ist als Pseudonym. Weitere Angaben zu Ihrer Person sind für die Anzeige des Testergebnisses in der App nicht erforderlich. Sie erhalten unabhängig eine Kopie des QR-Codes, der durch die Kommunikation Ihrer Smartphone in die App eingesendet werden kann. Nur hinsichtlich der Weitergabe des Testergebnisses mit Ihrer App möglich. Mit Ihrer Einwilligung können Sie durch Ihr Smartphone mit Hilfe der App abrufen. Ihr Testergebnis wird automatisch zum Zweck der Warnung an andere App-Nutzer übertragen. Bitte beachten Sie, dass aufgrund der besonderen Herausforderung, eine zuverlässige Warnung jederzeit mit Wirkung für die Zukunft zu gewährleisten, eine Löschung Ihrer Daten mit Hilfe der App nicht möglich ist. Ihre Einwilligung ist für die Nutzung der App erforderlich. Ihre Einwilligung ist für die Nutzung der App erforderlich. Ihre Einwilligung ist für die Nutzung der App erforderlich.

Scannen Sie diesen QR-Code



Falk Sippach: "CWA unter der Lupe"

embarc.de

16

16

Corona-Warn-App  
The official COVID-19 exposure notification app for Germany.  
https://coronawarn.app corona-warn-app.opensource@sap... Verified

Repositories 12 Packages People 56 Projects

Find a repository... Type: All Language: All

**cwa-app-ios**  
Native iOS app using the exposure notification framework from Apple.  
Swift 248 1,510 46 (1 issue needs help) 3 Updated 14 hours ago

**cwa-app-android**  
Native Android app using the Apple/Google exposure notification API.  
Kotlin Apache-2.0 458 2,139 93 (2 issues need help) 3 Updated 18 hours ago

**cwa-server**  
Backend implementation for the Apple/Google exposure notification API.  
corona coronavirus covid-19 covid19 cwa-server

Top languages  
Java Kotlin TeX Swift FreeMarker

People 56 >

Falk Sippach: "CWA unter der Lupe" embarc.de 17

17

**Auftraggeber** Die Bundesregierung

**Herausgeber** ROBERT KOCH INSTITUT

**Entwicklung** SAP T

**Berater** Fraunhofer CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Bundesamt für Sicherheit in der Informationstechnik

BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Falk Sippach: "CWA unter der Lupe" embarc.de 18

18

## Mission Statement (für diesen Vortrag)



- Klären, was **architekturelevante Anforderungen** sind.
- Einblicke geben in die Architektur der **Corona-Warn-App**.
- **Stärken, Risiken und Kompromisse** der gewählten Architektur der CWA kennenlernen.



## Agenda

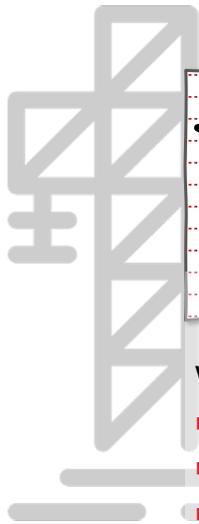


- 1 Einstieg und Motivation
- 2 Architekturelevante Anforderungen**
- 3 Lösungsansätze
- 4 Stärken, Risiken und Kompromisse
- 5 Ausblick und weitere Informationen

**2**



## Was ist Softwarearchitektur?



Softwarearchitektur :=

$\Sigma$  wichtige Entscheidungen

wichtig :=

- fundamental (betrifft viele)
- im weiteren Verlauf nur schwer zu ändern
- entscheidend für den Erfolg des Softwaresystems



Falk Sippach: "CWA unter der Lupe"

embarc.de

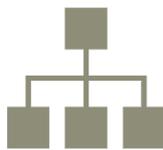
21

21

## Themen für Entscheidungen

### Zerlegung

Welcher Architekturstil?  
Wie zerfällt die Anwendung?  
Teilsysteme, Module,  
Komponentenbildung,  
Abhängigkeiten ...



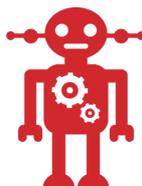
### Zielumgebung

Wo läuft die Software?  
Beim Endanwender, im  
eigenen Rechenzentrum,  
Cloud, Verteilung,  
Virtualisierung ...



### Technologie-Stack

Was setzen wir ein?  
Programmiersprache(n)  
Bibliotheken, Frameworks,  
Middleware,  
Querschnittsthemen ....



### Vorgehen

Wie arbeiten wir?  
Planen, Entwickeln, Testen,  
Bauen, Dokumentieren,  
Ausliefern, Nachjustieren,  
...



Falk Sippach: "CWA unter der Lupe"

embarc.de

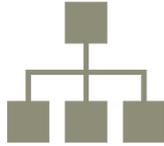
22

22

## CWA – Konkrete Entscheidungen

### Zerlegung

Client/Server mit Apps und Backend-Server als verteilte Menge einzeln deploybarer Services, **fachlich zerlegt** (Test-ergebnisse, Verifikation ...)



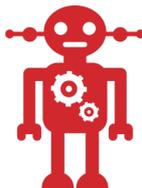
### Zielumgebung

Clients: **Smartphones** der Endnutzer, Backend: **Kubernetes in der Telekom-Cloud ...**



### Technologie-Stack

**Native Apps** in Swift und Kotlin auf iOS und Android. Backend in **Java mit Spring Boot**, Postgres, ...



### Vorgehen

Entwicklung als **Open Source**, Quelltexte in **GitHub**, **Dokumentation** in Markdown, automatisierte **Tests** ...



Falk Sippach: "CWA unter der Lupe"

embarc.de

23

23

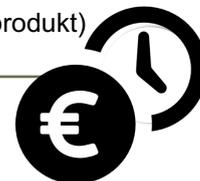
## Einflüsse auf Entscheidungen



### Rahmenbedingungen

Technisch (z.B. Datenbankprodukt)  
Organisatorisch (z.B. Team)

- schränken die Lösung ein
- schließen Optionen aus



Falk Sippach: "CWA unter der Lupe"

embarc.de

24

24

## Zentrale Rahmenbedingungen Corona-Warn-App



### Technisch

- Betrieb in der **Cloud**
- **Native mobile** Clients
- Einsatz des **Exposure Notification Framework**

### Organisatorisch

- **Große Medienaufmerksamkeit**, gewisse **Skepsis** am Mehrwert innerhalb der Bevölkerung
- Konsortium aus **zwei Auftragnehmern** (SAP und Deutsche Telekom)
- **Enger Zeitrahmen**
- Hoher **politischer Druck**, viele Parteien involviert (Ministerien, Behörden, RKI)
- **Hohe Datenschutzerfordernungen**



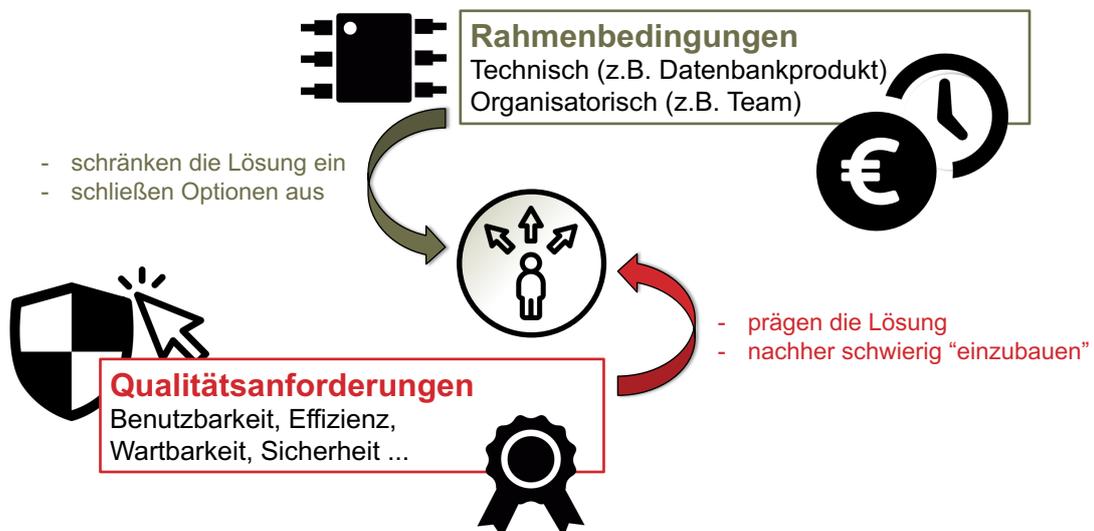
Falk Sippach: "CWA unter der Lupe"

embarc.de

25

25

## Einflüsse auf Entscheidungen



Falk Sippach: "CWA unter der Lupe"

embarc.de

26

26

## Qualitätsmerkmale

Begriffe  
nach  
ISO 25010 



**Benutzbarkeit**  
(Usability)

Ist die Software intuitiv zu bedienen, leicht zu erlernen, attraktiv?



**Portabilität**  
(Portability)

Ist die Software leicht auf andere Zielumgebungen (z.B. anderes OS) übertragbar?



**Funktionale Eignung**  
(Functional Suitability)

Sind die berechneten Ergebnisse genau genug / exakt, ist die Funktionalität angemessen? ...



**Effizienz**  
(Performance)

Antwortet die Software schnell, hat sie einen hohen Durchsatz, einen geringen Ressourcenverbrauch? ...



**Kompatibilität**  
(Compatibility)

Ist die Software konform zu Standards, arbeitet sie gut mit anderen zusammen?



**Zuverlässigkeit**  
(Reliability)

Ist das System verfügbar, tolerant gegenüber Fehlern, nach Abstürzen schnell wieder hergestellt? ...



**Sicherheit**  
(Security)

Ist das System sicher vor Angriffen? Sind Daten und Funktion vor unberechtigtem Zugriff geschützt? ...



**Wartbarkeit**  
(Maintainability)

Ist die Software leicht zu ändern, erweitern, testen, verstehen? Lassen sich Teile wiederverwenden? ...



Falk Sippach: "CWA unter der Lupe"

embarc.de



27

## Top-Qualitätsziele Corona-Warn-App

Ziel	Beschreibung
 <b>Höchster Datenschutz</b>	Der Schutz der personenbezogenen Daten hat oberste Priorität. ( <i>Sicherheit</i> )
 <b>Effektive Warnfunktionalität</b>	Die App ist ein effektiver Baustein bei der Pandemie-Bekämpfung. ( <i>Funktionale Eignung</i> )
 <b>Attraktive Lösung für App-Nutzer</b>	Die App ist leicht zu installieren sowie intuitiv und effizient zu bedienen. ( <i>Benutzbarkeit</i> )
 <b>Hohe Zuverlässigkeit</b>	Die Lösung geht mit Lastspitzen wegen hoher Nutzer- oder Infektionszahlen ebenso souverän um, wie mit böswilligen Angriffen. ( <i>Zuverlässigkeit</i> )
 <b>Gute Änderbarkeit</b>	Die Software lässt sich leicht anpassen, wenn z. B. Nutzer/-innen oder neue Forschungsergebnisse es erfordern. ( <i>Wartbarkeit/Erweiterbarkeit</i> )

Die Reihenfolge gibt Orientierung bezüglich der Wichtigkeit.



Falk Sippach: "CWA unter der Lupe"

embarc.de

28

28

## Agenda



- 1 Einstieg und Motivation
- 2 Architekturelevante Anforderungen
- 3 Lösungsansätze**
- 4 Stärken, Risiken und Kompromisse
- 5 Ausblick und weitere Informationen

# 3



## Mission Statement



Die **Corona-Warn-App** ist eine App, die hilft, **Infektionsketten** des SARS-CoV-2 (COVID-19-Auslöser) in Deutschland **nachzuverfolgen** und zu **unterbrechen**.

Die App basiert auf Technologien mit einem **dezentralisierten Ansatz** und informiert Personen, wenn sie mit einer infizierten Person in Kontakt standen.

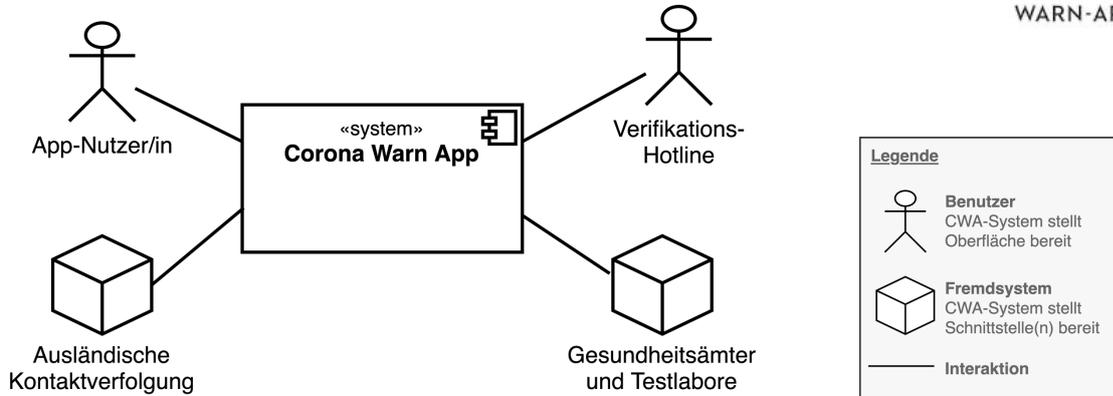
**Transparenz** ist von entscheidender **Bedeutung**, um die Bevölkerung zu schützen und die **Akzeptanz zu erhöhen**.

Quelle: <https://www.coronawarn.app/de/>



## Kontextabgrenzung

Dieser fachliche Systemkontext zeigt das Corona-Warn-App-System im Zusammenspiel mit den wichtigsten Benutzern und Fremdsystemen.



## Fachlicher Systemkontext, Akteure

Kurze Erläuterungen zu den Benutzern und Fremdsystemen

Akteur	Beschreibung
App-Nutzer/in	Erhält Informationen über mögliche Begegnungen mit infizierten Personen und eigene Testergebnisse. Verifiziert eigene Testergebnisse und warnt so freiwillig andere.
Verifikations-Hotline	Unterstützt App-Nutzer/innen bei der Freischaltung positiver Testergebnisse ("teleTAN").
Gesundheitsämter und Testlabore	Liefern anonymisierte Testergebnisse an das System.
Ausländische Kontaktverfolgungen	Austausch mit dezentralen Anwendungen anderer Länder zur grenzüberschreitenden Ermittlung von Kontakten.



## Lösungsstrategie Corona-Warn-App

Ziel	Passende Lösungsansätze (Auswahl)
<b>Höchster Datenschutz</b>	<ul style="list-style-type: none"> <li>• Speicherung der <b>Daten lokal</b></li> <li>• <b>Verschlüsselung</b> aller Bewegungsdaten</li> <li>• Senden der Daten nur <b>nach Aufforderung</b></li> <li>• <b>Transparente</b> Entwicklung (Open Source)</li> </ul>
<b>Effektive Warnfunktionalität</b>	<ul style="list-style-type: none"> <li>• Verwendung <b>Exposure Notification Framework</b></li> <li>• <b>Digitale Abläufe</b> bevorzugt</li> <li>• Optionales, manuelles <b>Kontakt-Tagebuch</b></li> </ul>
<b>Attraktive Lösung für App-Nutzer</b>	<ul style="list-style-type: none"> <li>• <b>Native Clients</b> (L&amp;F)</li> <li>• <b>Übersichtliche</b> Gestaltung und <b>simple</b> Bedienung</li> </ul>
<b>Hohe Zuverlässigkeit</b>	<ul style="list-style-type: none"> <li>• <b>Microservices</b>, Docker, Kubernetes, <b>Public Cloud</b></li> <li>• hohe <b>Testabdeckung</b> und <b>automatisierte Builds</b></li> <li>• Bereitstellung von zu lesenden Daten über <b>CDN</b></li> </ul>
<b>Gute Änderbarkeit</b>	<ul style="list-style-type: none"> <li>• Hoher <b>Modularisierungsgrad</b></li> <li>• <b>Open Source</b> Projekt, gute <b>Dokumentation</b></li> <li>• Verwendung von <b>Standard &amp; Open Source</b> Libraries</li> <li>• Konsortium von <b>mehreren Auftragnehmern</b></li> <li>• <b>Code-Qualität</b> (SonarQube, SwiftLint, Checkstyle, ...)</li> </ul>

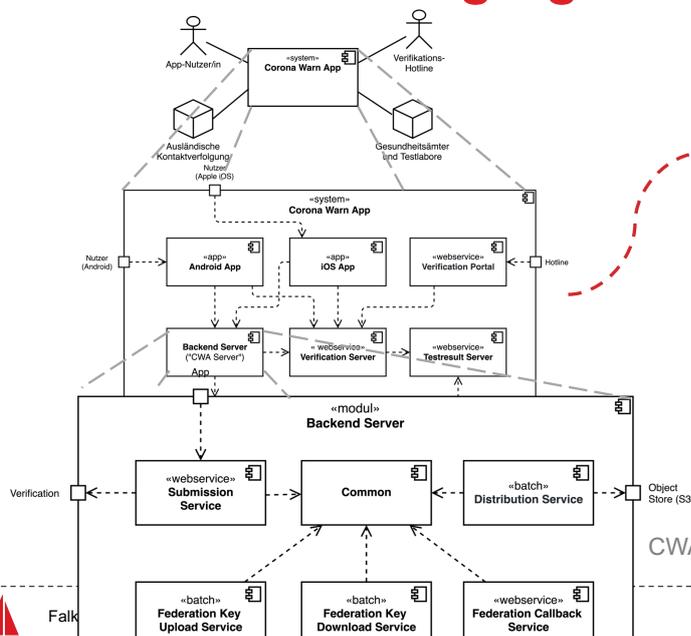
Falk Sippach: "CWA unter der Lupe"

embarc.de

33

33

## Tatsächliche Zerlegung im Quelltext



„Bausteinsicht, Ebene 1“

GitHub-Repositories

[https://github.com/corona-warn-app/...](https://github.com/corona-warn-app/)

- cwa-app-android
- cwa-app-ios
- cwa-server („Backend“)
- cwa-testresult-server
- cwa-verification-server
- cwa-verification-portal

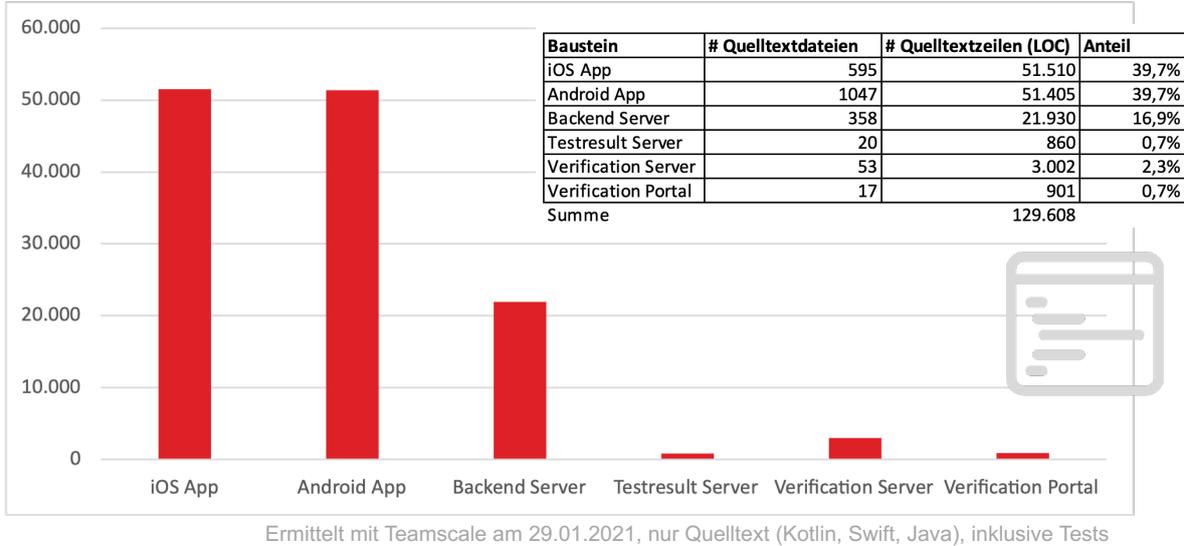
CWA-Server (Backend), Bausteinsicht, Ebene 2

Falk

34

34

## Umfang je Baustein auf Ebene 1



Falk Sippach: "CWA unter der Lupe"

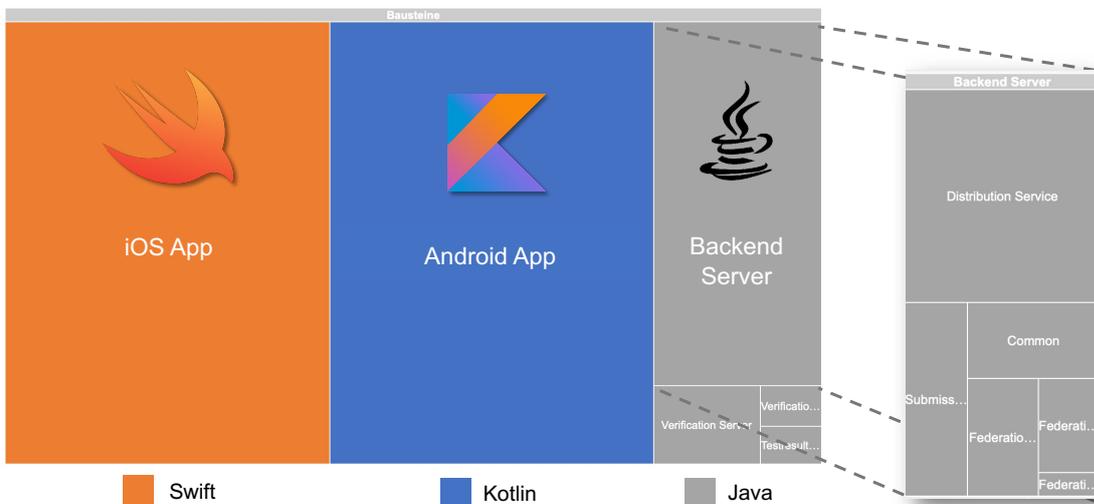
embarc.de

35

35

## Treemap zum Umfang inkl. Programmiersprachen

Die Fläche einer Kachel entspricht LOCs des Repositories, die Farbe der Programmiersprache.



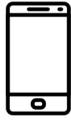
Falk Sippach: "CWA unter der Lupe"

embarc.de

36

36

## Technologie-Stack



- **Native Clients** in Swift bzw. Kotlin für iOS und Android
- **SQLite**



- **Java 11**
- **Spring Boot/Cloud/Data**
- Lombok, Guava, ...
- **REST, Protobuf**
- **OpenAPI, Micrometer**
- Liquibase



- Maven, Gradle
- **Docker, Kubernetes**
- **Open Telekom Cloud** (OpenStack)
- PostgreSQL, **S3, CDN**
- Keycloak



Falk Sippach: "CWA unter der Lupe"

embarc.de

37

37

## Agenda



- 1 Einstieg und Motivation
- 2 Architekturelevante Anforderungen
- 3 Lösungsansätze
- 4 Stärken, Risiken und Kompromisse**
- 5 Ausblick und weitere Informationen

# 4



Falk Sippach: "CWA unter der Lupe"

embarc.de

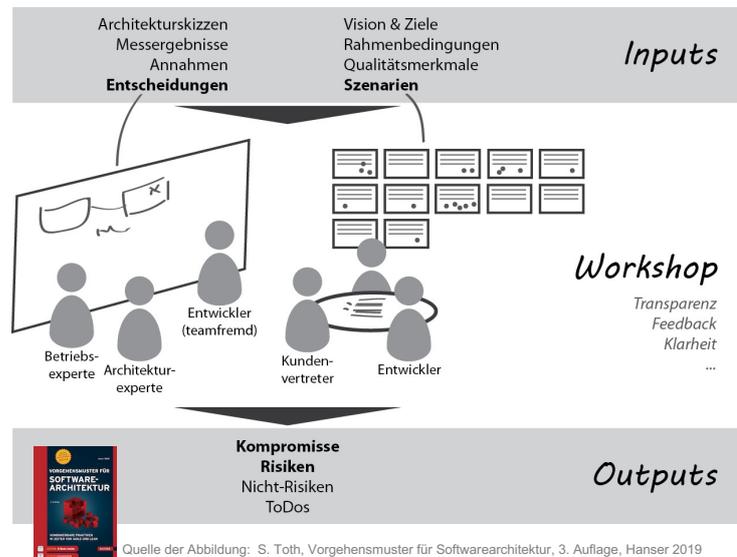
38

38

## Szenarienbasierte Bewertung

### Ablauf

- (1) Szenarien generieren
- (2) Szenarien priorisieren
- (3) Szenarien durchsprechen (der Reihe, nach Priorität)



## Was ist ein Szenario?

### Ein Qualitätsszenario (auch: Bewertungsszenario) ...

- ... ist ein kurzer Text (1-3 Sätze).
- ... beschreibt **beispielhaft** die Verwendung des Systems, und zwar so dass ein **Qualitätsmerkmal** die Hauptrolle spielt.



### Wie konkret?



- Man muss sinnvoll drüber reden können.
- Man muss es (theoretisch) überprüfen können.
- (Kein Abnahmekriterium, kein Testfall!)



# Brainstorming – analog oder digital

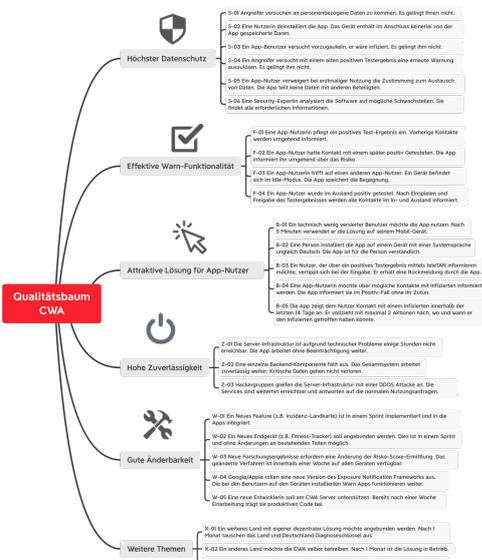
## In Präsenz: Post-its



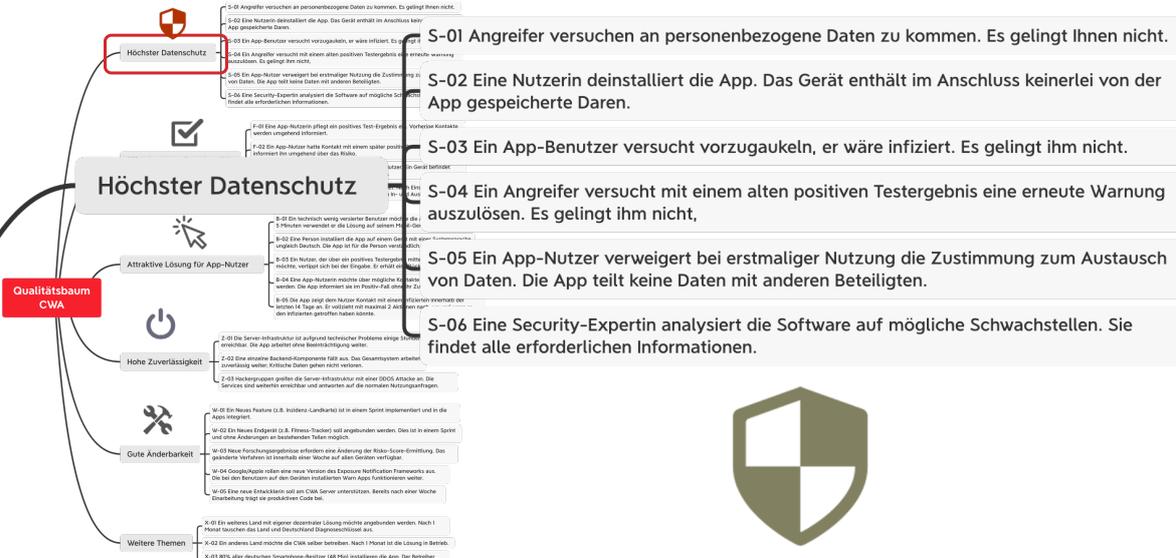
## Remote: Digitale Whiteboards (miro, Mural, ...)



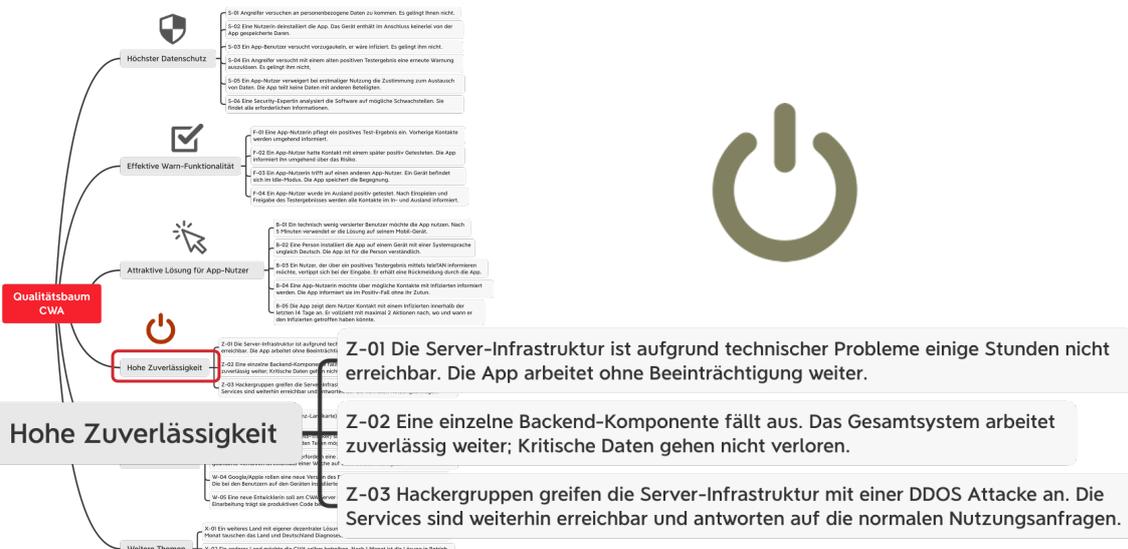
# Ergebnis: Qualitätsbaum mit Szenarien



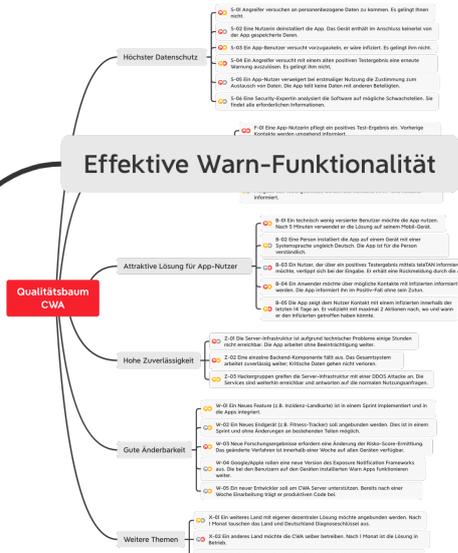
## Ergebnis: Qualitätsbaum mit Szenarien



## Ergebnis: Qualitätsbaum mit Szenarien



# Beispiel: Unser CWA-Qualitätsbaum, priorisiert

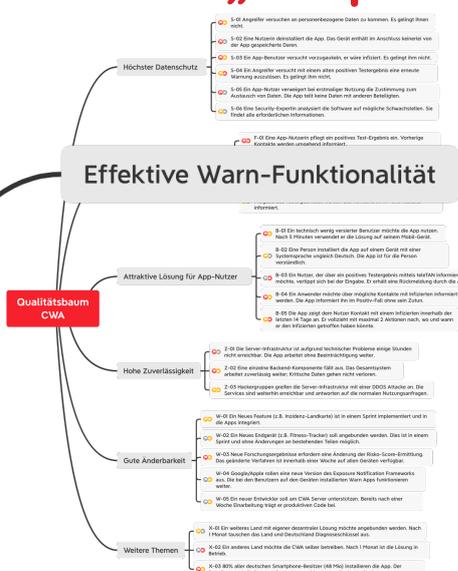


- F-01 Eine App-Nutzerin pflegt ein positives Test-Ergebnis ein. Vorherige Kontakte werden umgehend informiert.
- F-02 Ein App-Nutzer hatte Kontakt mit einem später positiv Getesteten. Die App informiert ihn umgehend über das Risiko.
- F-03 Ein App-Nutzerin trifft auf einen anderen App-Nutzer. Ein Gerät befindet sich im Idle-Modus. Die App speichert die Begegnung.
- F-04 Ein App-Nutzer wurde im Ausland positiv getestet. Nach Einspielen und Freigabe des Testergebnisses werden alle Kontakte im In- und Ausland informiert.

**Legende für Priorität**

- Fachliche Wichtigkeit
- Technische Schwierigkeit
- Rot: Hoch
- Gelb: Mittel
- Grau: Niedrig

# Szenario „rauspicken“: F-01

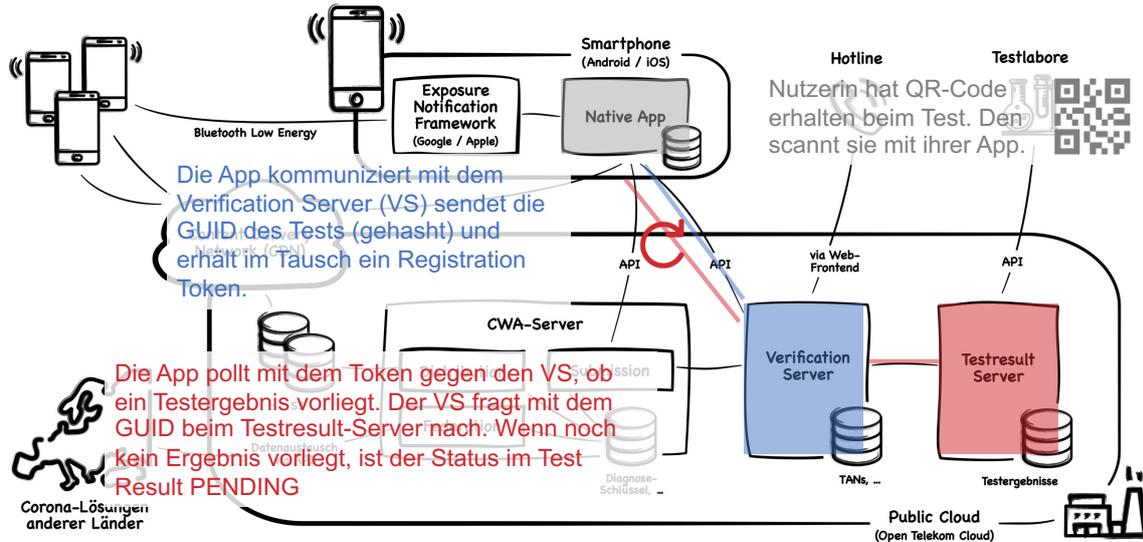


- F-01 Eine App-Nutzerin pflegt ein positives Test-Ergebnis ein. Vorherige Kontakte werden umgehend informiert.
- F-02 Ein App-Nutzer hatte Kontakt mit einem später positiv Getesteten. Die App informiert ihn umgehend über das Risiko.
- F-03 Ein App-Nutzerin trifft auf einen anderen App-Nutzer. Ein Gerät befindet sich im Idle-Modus. Die App speichert die Begegnung.
- F-04 Ein App-Nutzer wurde im Ausland positiv getestet. Nach Einspielen und Freigabe des Testergebnisses werden alle Kontakte im In- und Ausland informiert.



F-01 Eine App-Nutzerin pflegt ein positives Test-Ergebnis ein. Vorherige Kontakte werden umgehend informiert.

## Szenario F-01: Schritte entlang des Überblicks



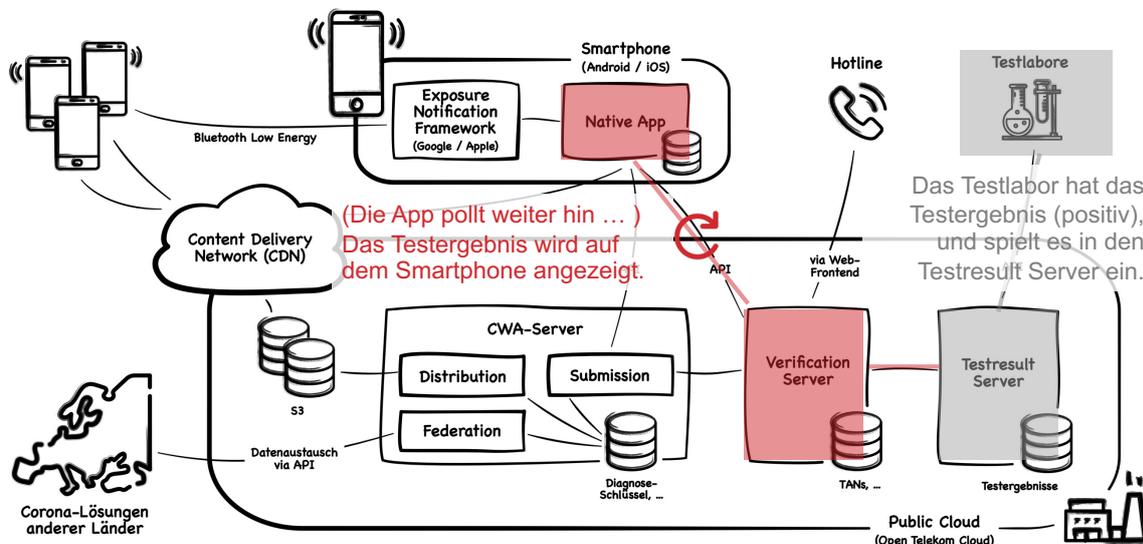
Falk Sippach: "CWA unter der Lupe"

embarc.de

47

47

## Szenario F-01: Schritte entlang des Überblicks



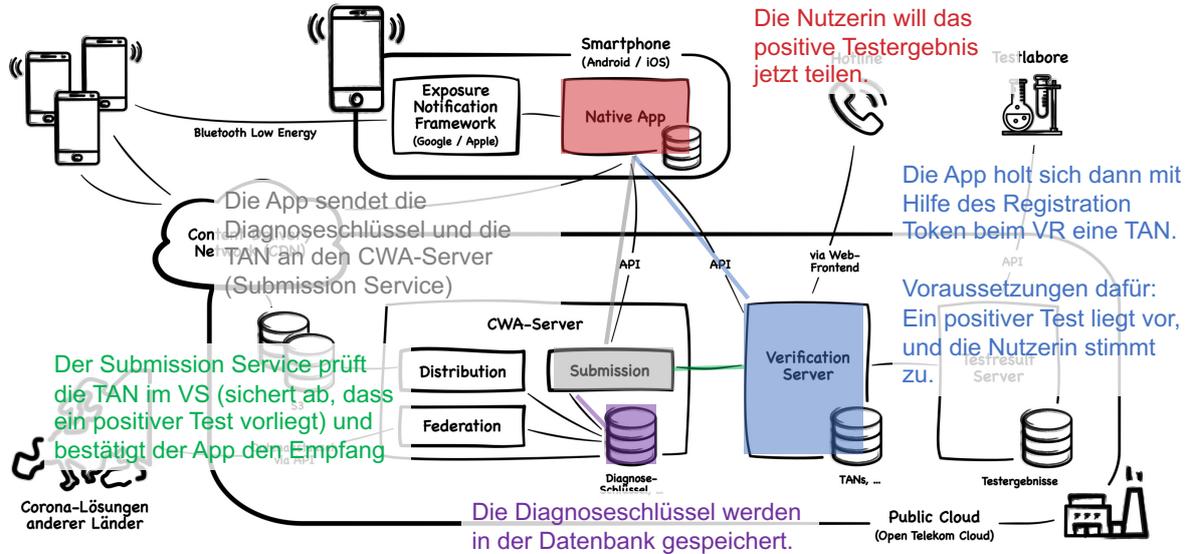
Falk Sippach: "CWA unter der Lupe"

embarc.de

48

48

## Szenario F-01: Schritte entlang des Überblicks



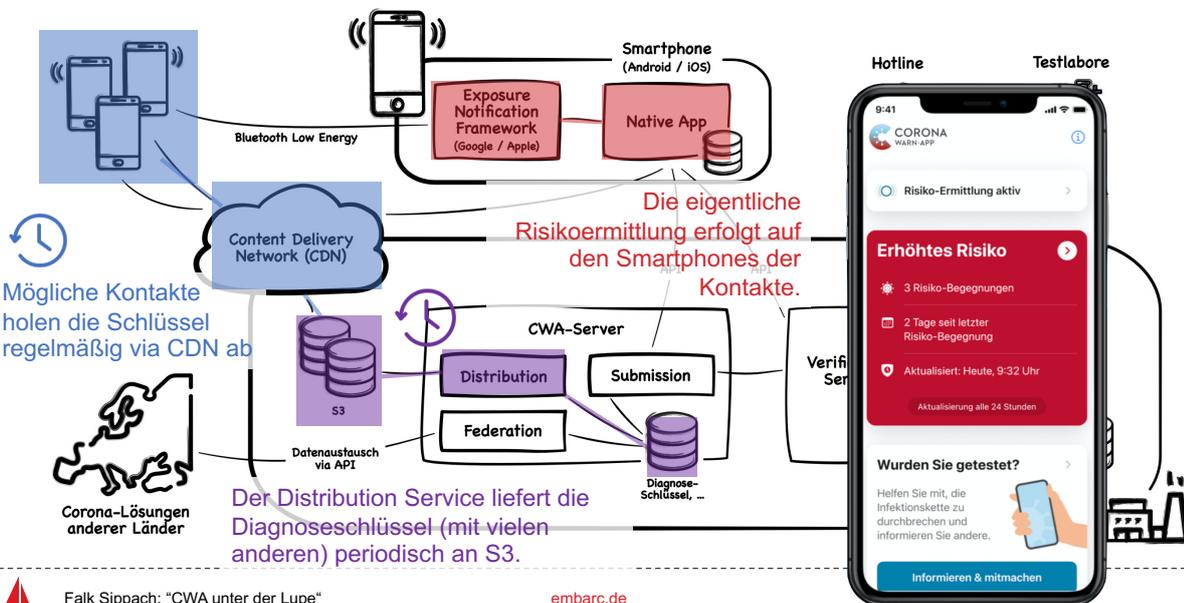
Falk Sippach: "CWA unter der Lupe"

embarc.de

49

49

## Szenario F-01: Schritte entlang des Überblicks



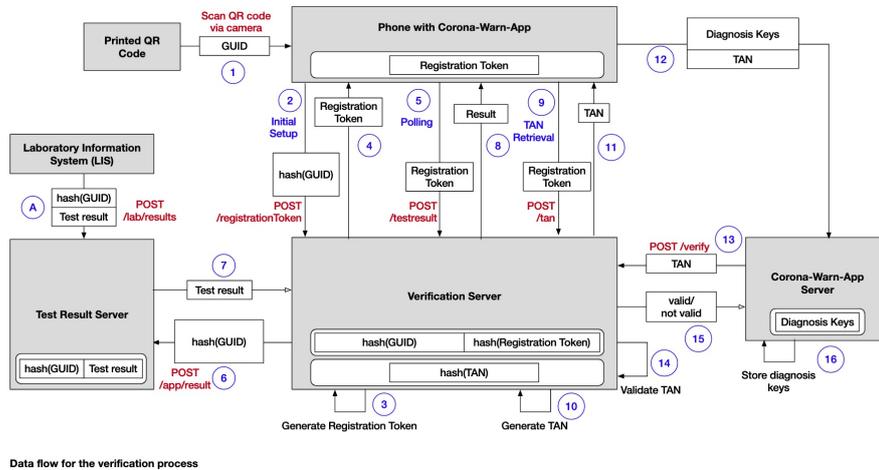
Falk Sippach: "CWA unter der Lupe"

embarc.de

50

50

## Zum ganz genau nachlesen ...



Data flow for the verification process

<https://github.com/corona-warn-app/cwa-verification-server/blob/master/docs/architecture-overview.md>



51

## Ausgewählte Ergebnisse zu Szenario F-01

F-01 Eine App-Nutzerin pflegt ein positives Test-Ergebnis ein. Vorherige Kontakte werden umgehend informiert.

### Kompromisse

- Apps der Kontakte aktualisieren via CDN nur ab und an (+) **effiziente Nutzung / Bandbreite** des Smartphone (-) nicht "umgehend", **Verzögerung bei Warnungen**
- explizite Einwilligung der Nutzerin erforderlich (-) **Benutzbarkeit** (+) **Datenschutz**
- Registration Token und TAN „verkomplizieren“ den Ablauf (TAN wichtig für Sicherheits-Szenarien S-03 und S-04)

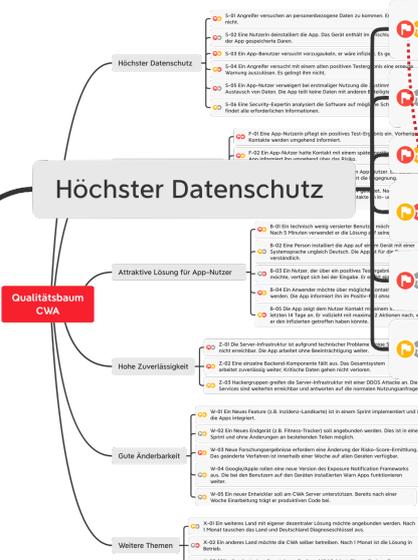
### Risiken

- Wenn das Testlabor das Ergebnis nicht oder **zeitlich stark verzögert einspielt**, kann die Nutzerin erst **spät freigeben**, oder gar nicht, oder **gibt irgendwann resigniert auf**.
- Periodische Erzeugung der Daten kann Liefern der Diagnoseschlüssel an S3 verzögern (gefährdet „umgehend“) – Fragen: Wie oft passiert das? Wie lange dauert ein Lauf?



52

## Szenario 2: S-01



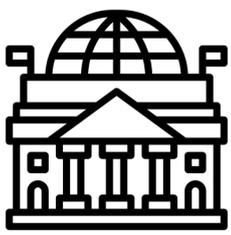
- S-01 Angreifer versuchen an personenbezogene Daten zu kommen. Es gelingt Ihnen nicht.
- S-02 Eine Nutzerin deinstalliert die App. Das Gerät enthält im Anschluss keinerlei von der App gespeicherte Daten.
- S-03 Ein App-Benutzer versucht vorzugaukeln, er wäre infiziert. Es gelingt ihm nicht.
- S-04 Ein Angreifer versucht mit einem alten positiven Testergebnis eine erneute Warnung auszulösen. Es gelingt ihm nicht.
- S-05 Ein App-Nutzer verweigert bei erstmaliger Nutzung die Zustimmung zum Austausch von Daten. Die App teilt keine Daten mit anderen Beteiligten.
- S-06 Eine Security-Expertin analysiert die Software auf mögliche Schwachstellen. Sie findet alle erforderlichen Informationen.



S-01 Angreifer versuchen an personenbezogene Daten zu kommen. Es gelingt Ihnen nicht.

## Szenario 2 (S-01): Nachschärfen

S-01 Angreifer versuchen an personenbezogene Daten zu kommen. Es gelingt Ihnen nicht.



Wer "greift an"?

Gute oder schlechte Absichten?



## Szenario 2 (S-01): Nachschärfen

S-01 Angreifer versuchen an personenbezogene Daten zu kommen. Es gelingt Ihnen nicht.

### Was sind personenbezogene Daten?



- "Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen". (Artikel 4 DSGVO)
- **Identifiziert** = Zuordnung der Daten ohne Umweg, direkter Bezug herstellbar
- **Identifizierbar** = Zuordnung mit Zusatzwissen

### Wer nutzt die App überhaupt?



- 22 Millionen Installationen der App
- **18 bis 20 Millionen** aktive Nutzer
- mehr als **zwei Millionen Laborergebnisse** über die App übermittelt
- rund **53.000 Nutzer** haben ihr positives Testergebnis **über die App geteilt**.

Laut Bundesregierung (November 2020)

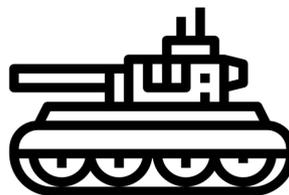


## Szenario 2 (S-01): Nachschärfen

S-01 Angreifer *versuchen* an personenbezogene Daten zu *kommen*. Es gelingt Ihnen nicht.

### Potentielle Angriffsvektoren (in der Theorie!)

ID-Scanner



ID-Bomber

ID-Repeater



## Szenario 2 (S-01): Nachschärfen

S-01 Angreifer versuchen an personenbezogene Daten zu kommen. *Es gelingt Ihnen nicht.*

### Was darf nicht passieren?

Personen tracken

Verpflichtung zur App an bestimmten Orten und Veranstaltungen

Namen von Infizierten ermitteln



Falschmeldungen verbreiten

Gesundheitsamt wird direkt über erhöhtes Risiko informiert und ordnet Quarantäne an



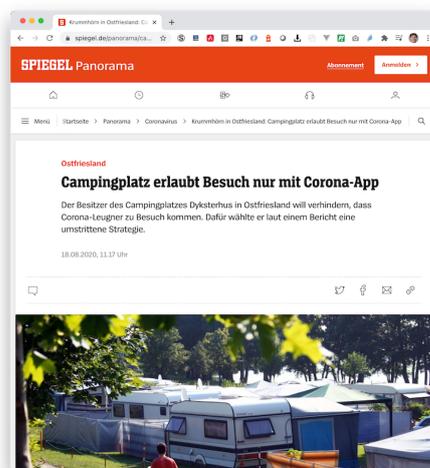
Falk Sippach: "CWA unter der Lupe"

embarc.de

57

57

## CWA als Must-Have?



„Nur wer die Corona-Warn-App installiert hat, **darf anreisen**: Ein Betreiber eines Campingplatzes in Niedersachsen versucht ab diesem Dienstag mit einer drastischen Strategie, **Urlauber fernzuhalten**, die aus seiner Sicht das **Coronavirus nicht ernst nehmen**. Angesichts der steigenden Zahl der Infizierten wolle er seine **Gäste, seine Familie und sich selbst schützen**, sagte Campingplatz-Chef [...]“

<https://www.spiegel.de/panorama/camping-platz-erlaubt-besuch-nur-mit-corona-app-a-0c6bfcfe-5bcb-463a-b670-790030560d80#>



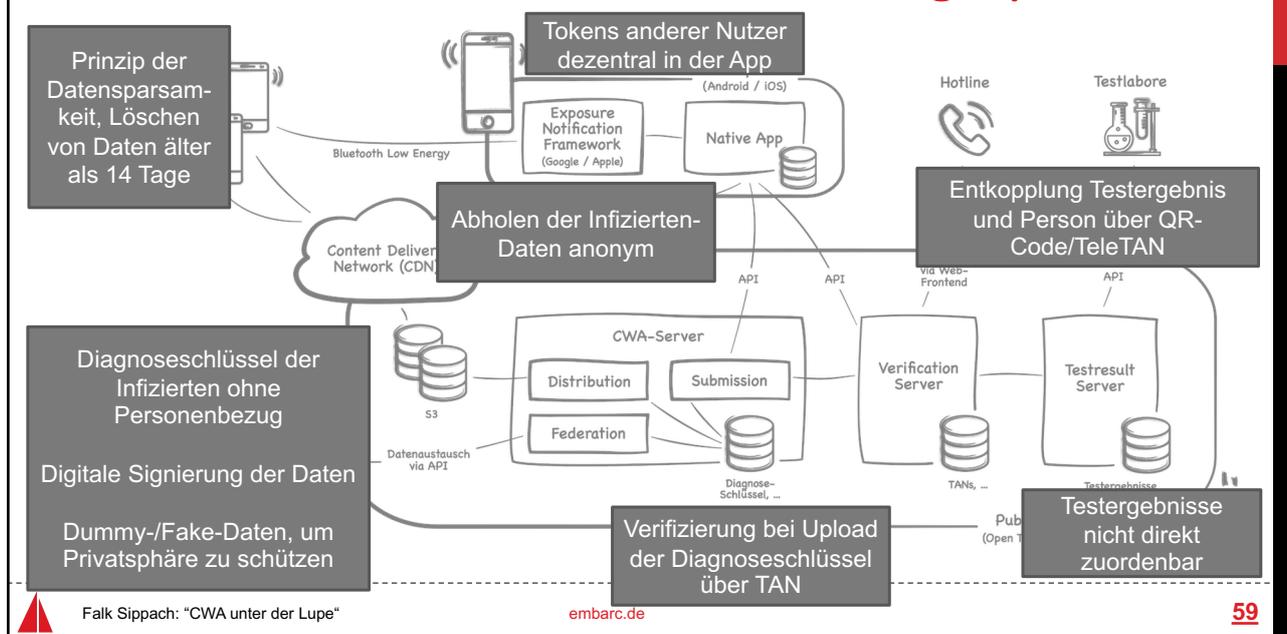
Falk Sippach: "CWA unter der Lupe"

embarc.de

58

58

## Szenario S-01: Wo/Wie werden Daten gespeichert?



59

## Ausgewählte Ergebnisse zu Szenario S-01

S-01 Angreifer versuchen an personenbezogene Daten zu kommen. Es gelingt Ihnen nicht.

### Kompromisse

- Offenlegung des Quelltextes
  - (+) **schaftt Vertrauen**
  - (-) **zeigt ggf. Schwachstellen** auf
- Gesundheitsämter haben keinen direkten Zugriff auf personenbezogene Daten
  - (+) **keine Bevormundung/Überwachung**
  - (-) Staat ist auf **freiwillige Mithilfe** angewiesen
- Keine Möglichkeit, in den letzten Tagen getroffene Personen zu ermitteln (Pull, kein Push)
  - (-) Kontakte muss jeder **selbst dokumentieren**
  - (+) CWA bietet ein digitales Kontakt-Tagebuch an

### Stärken

- + **Dezentrale Speicherung** auf den Smartphones
- + **Datensparsamkeit** (keine direkte Speicherung von personenbezogenen Daten)
- + **Regelmäßige Löschen** (14 Tage)
- + **Fake-Daten**, um bei geringer Datenmenge keine Rückschlüsse zu erlauben
- + Generierung von Schlüsseln, **rollierende Tokens**
- Wirksamkeit wegen hohen Datenschutzanforderungen zu gering?
  - (+) **Chaos Computer Club lobt** die CWA explizit
  - (-) Politiker möchten den **Datenschutz** für eine bessere Wirkung **opfern**
- eingeschränkte Möglichkeiten zur Auswertung der Benutzung
  - (+) **Datenschutz**
  - (-) **Interessante Statistiken** zur Nutzung **nicht möglich**

Falk Sippach: "CWA unter der Lupe"

embarc.de

60

60

## Szenario 3: Z-02



Z-02 Eine einzelne Backend-Komponente fällt aus. Das Gesamtsystem arbeitet zuverlässig weiter. Kritische Daten gehen nicht verloren.



Z-01 Die Server-Infrastruktur ist aufgrund technischer Probleme einige Stunden nicht erreichbar. Die App arbeitet ohne Beeinträchtigung weiter.

Z-02 Eine einzelne Backend-Komponente fällt aus. Das Gesamtsystem arbeitet zuverlässig weiter; Kritische Daten gehen nicht verloren.

Z-03 Hackergruppen greifen die Server-Infrastruktur mit einer DDOS Attacke an. Die Services sind weiterhin erreichbar und antworten auf die normalen Nutzungsanfragen.



## Ausgewählte Ergebnisse zu Szenario Z-02

Z-02 Eine einzelne Backend-Komponente fällt aus. Das Gesamtsystem arbeitet zuverlässig weiter. Kritische Daten gehen nicht verloren.

### Stärken

- + Apps funktionieren auch **ohne Backends** (sammeln Daten)
- + **"Kleine" Services** mit meist eigener Datenhaltung
- + **Containerisierung** der Services und Orchestrierung über Kubernetes
- + **Public Cloud** inklusive horizontale Skalierbarkeit und Redundanz
- + Häufige Lesezugriffe über **CDN entkoppelt** (Caching, Skalierbarkeit)

### Kompromisse

- Synchroner Kommunikation App zum Server  
(+) Benutzer erhalten **sofort Rückmeldung**  
(-) hat ggf. **Auswirkungen auf Zuverlässigkeit**
- Synchroner Kommunikation Labore zum Test-Result-Server  
(+) **einfacher aufzurufen** für die Labore  
(-) **Akzeptanz bei Benutzern sinkt**, wenn die Ergebnisse nicht in der App angezeigt werden



## Agenda



- 1 Einstieg und Motivation
- 2 Architekturelevante Anforderungen
- 3 Lösungsansätze
- 4 Stärken, Risiken und Kompromisse
- 5 Ausblick und weitere Informationen**

# 5

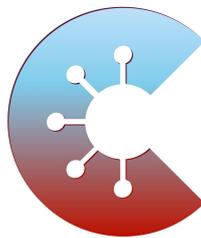


Falk Sippach: "CWA unter der Lupe"

embarc.de

63

63



# Gemeinsam Corona bekämpfen

<https://www.coronawarn.app>



Falk Sippach: "CWA unter der Lupe"

embarc.de

64

64

## Stetige Weiterentwicklung



Falk Sippach: "CWA unter der Lupe"

embarc.de

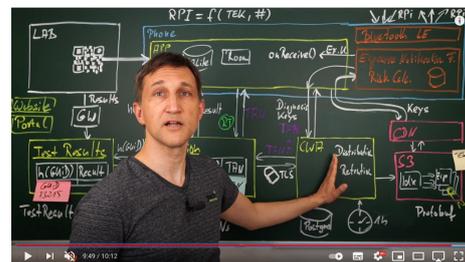
65

65

## Video-Tipp zur Corona-Warn-App

Video-Serie zur Funktionsweise der CWA von Thomas Bayer auf YouTube.

„Technischer Blick auf die Corona Warn App und ihre Backend-Systeme. Videos zur Funktionsweise, Softwarearchitektur, Protokollen, Sicherheit.“



#1: Wie funktioniert die Corona Warn App (CWA)?

<https://www.youtube.com/watch?v=MEQ0wzk1Cp8>

#2: Softwarearchitektur der Corona App

<https://www.youtube.com/watch?v=ytgISxeTPyU>

#3: Kommunikation mit Backend-Servern in der Cloud #1

<https://www.youtube.com/watch?v=RKoBcsCA5ts>

#4: Corona App Technik: Backend, Datenbank, S3, Cloud Teil #2

<https://www.youtube.com/watch?v=7mebVNWcGxU>



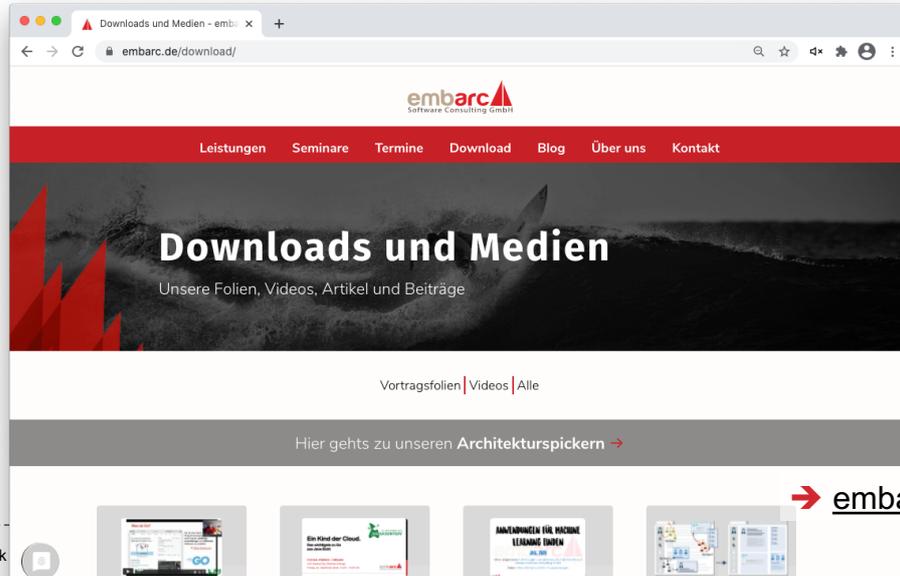
Falk Sippach: "CWA unter der Lupe"

embarc.de

66

66

## Folien von heute als PDF zum Download



→ [embarc.de/download/](https://embarc.de/download/)

## Flyer Architekturüberblick zur CWA zum Download

### [E: Bewertung & Ausblick]

#### Ausgewählte Kompromisse

Der Entwurf der CWA geht bewusst Trade-offs ein und balanciert Qualitätsziele aus.

Explizite Freigabe positiver Testergebnisse durch Nutzer:in erforderlich

- erhöht Vertrauen in die Lösung
- reduziert effektive Warnfunktionalität

Verteilte Anwendung auf dem Backend

- gut für Datenschutz (Freigabe der Daten)
- verfügbar(er) im Fall von Teilschleifern
- schwieriger zu entwickeln und zu betreiben

Vergleichsweise hohe Kopplung der Microservices

- einfacher umzusetzen, schneller am Markt
- erschwert unabhängige Entwicklung
- reduziert oder behindert Zuverlässigkeit

Auslasten der Diagnoseschlüssel über CDN im Batch, Aktualisierung durch Apps in Intervallen

- spart Ressourcen, vor allen an den Endgeräten
- höchst, erhöht Zuverlässigkeit
- Zwangslegung bei Risikovermittlung

#### Nächste Schritte für die CWA

Auf Basis dieser Lösungsarchitektur sind weitere Features angelegt, konzipiert oder bereits umgesetzt, z.B.

- lokales Kontaktüberblick (Nutzung optional)
- Anzeige ausgewählter Kennzahlen zum Infektionsgeschehen (Berstellung RKI)
- Eventgesteuerte Entschicken mit QR-Code, Erkennen sogenannter Cluster
- Integration von Schnelltestergebnissen
- Anzeige eines digitalen Impfnachweises

#### Weitere Informationen

zur Corona-Warn-App:  
Homepage des Open-Source-Projektes:  
[www.coronawarn.app/de/](https://www.coronawarn.app/de/)

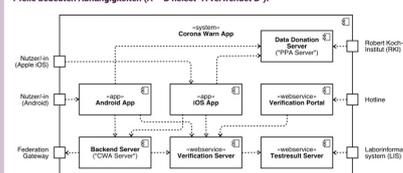
Qualitäts- und Dokumentations auf GitHub:  
[github.com/corona-warn-app](https://github.com/corona-warn-app)

zum Anfertigen von Architekturüberblicken:  
Gesammeltes Material (Videos, E-Books, ...)  
[www.embarc.de/architektur-ueberblicke/](https://www.embarc.de/architektur-ueberblicke/)

### [D: Eintauchen in die Corona-Warn-App]

#### Zerlegung auf oberster Ebene

Das Diagramm zeigt die wichtigsten Bausteine der CWA gemäss der Struktur des Quelltextes. Die Pfeile bedeuten Abhängigkeiten (A - B heisst 'A verwendet B').



Die GitHub-Repositorien liegen unterhalb von [github.com/corona-warn-app/](https://github.com/corona-warn-app/)

iOS App - Native App für iPhones. Gibt Testergebnisse frei. Ermittelt Infektionsrisiko anhand von Diagnoseschlüsseln. Sendet Daten.

Android App - Native Android App, analog zur iOS App.

Data Donation Server - Nimmt Nutzerdaten bei aktivierter Datenerhebung entgegen und speichert sie, ohne Rückschlüsse auf individuelle Personen zuzulassen. (PPA - Privacy Preserving Analytics).

Verification Portal - Ermöglicht die Erzeugung von sId/AnIs im Verification Server über ein einfaches Browser-Frontend.

Testresult Server - Empfängt und speichert die Testergebnisse von angeschlossenen Laboren.

Backend Server (CWA Server) - Nimmt die Diagnoseschlüssel positiv Getesteter entgegen und teilt sie mit anderen Nutzern über ein CDN, interagiert mit den Kontaktverfolgungen anderer Länder („Federation“).

Verification Server - Sichert ab, dass ein Nutzer der Meldung seines positiven Tests zugestimmt, und dass das Labor tatsächlich positiv getestet hat.

Testresult Server - Empfängt und speichert die Testergebnisse von angeschlossenen Laboren.

Verification Portal - Ermöglicht die Erzeugung von sId/AnIs im Verification Server über ein einfaches Browser-Frontend.

Data Donation Server - Nimmt Nutzerdaten bei aktivierter Datenerhebung entgegen und speichert sie, ohne Rückschlüsse auf individuelle Personen zuzulassen. (PPA - Privacy Preserving Analytics).

Android App - Native Android App, analog zur iOS App.

iOS App - Native App für iPhones. Gibt Testergebnisse frei. Ermittelt Infektionsrisiko anhand von Diagnoseschlüsseln. Sendet Daten.

Backend Server (CWA Server) - Nimmt die Diagnoseschlüssel positiv Getesteter entgegen und teilt sie mit anderen Nutzern über ein CDN, interagiert mit den Kontaktverfolgungen anderer Länder („Federation“).

Verification Server - Sichert ab, dass ein Nutzer der Meldung seines positiven Tests zugestimmt, und dass das Labor tatsächlich positiv getestet hat.

Testresult Server - Empfängt und speichert die Testergebnisse von angeschlossenen Laboren.

Verification Portal - Ermöglicht die Erzeugung von sId/AnIs im Verification Server über ein einfaches Browser-Frontend.

Data Donation Server - Nimmt Nutzerdaten bei aktivierter Datenerhebung entgegen und speichert sie, ohne Rückschlüsse auf individuelle Personen zuzulassen. (PPA - Privacy Preserving Analytics).

Android App - Native Android App, analog zur iOS App.

iOS App - Native App für iPhones. Gibt Testergebnisse frei. Ermittelt Infektionsrisiko anhand von Diagnoseschlüsseln. Sendet Daten.

Backend Server (CWA Server) - Nimmt die Diagnoseschlüssel positiv Getesteter entgegen und teilt sie mit anderen Nutzern über ein CDN, interagiert mit den Kontaktverfolgungen anderer Länder („Federation“).

Verification Server - Sichert ab, dass ein Nutzer der Meldung seines positiven Tests zugestimmt, und dass das Labor tatsächlich positiv getestet hat.

Testresult Server - Empfängt und speichert die Testergebnisse von angeschlossenen Laboren.

Verification Portal - Ermöglicht die Erzeugung von sId/AnIs im Verification Server über ein einfaches Browser-Frontend.

Data Donation Server - Nimmt Nutzerdaten bei aktivierter Datenerhebung entgegen und speichert sie, ohne Rückschlüsse auf individuelle Personen zuzulassen. (PPA - Privacy Preserving Analytics).

Android App - Native Android App, analog zur iOS App.

iOS App - Native App für iPhones. Gibt Testergebnisse frei. Ermittelt Infektionsrisiko anhand von Diagnoseschlüsseln. Sendet Daten.

Backend Server (CWA Server) - Nimmt die Diagnoseschlüssel positiv Getesteter entgegen und teilt sie mit anderen Nutzern über ein CDN, interagiert mit den Kontaktverfolgungen anderer Länder („Federation“).

Verification Server - Sichert ab, dass ein Nutzer der Meldung seines positiven Tests zugestimmt, und dass das Labor tatsächlich positiv getestet hat.

Testresult Server - Empfängt und speichert die Testergebnisse von angeschlossenen Laboren.

Verification Portal - Ermöglicht die Erzeugung von sId/AnIs im Verification Server über ein einfaches Browser-Frontend.

Data Donation Server - Nimmt Nutzerdaten bei aktivierter Datenerhebung entgegen und speichert sie, ohne Rückschlüsse auf individuelle Personen zuzulassen. (PPA - Privacy Preserving Analytics).

### Die deutsche Corona Warn-App

Ein prägnanter Überblick über die Softwarearchitektur der Gesamtlösung - Apps & Backend

Stand: April 2021

#### Architekturüberblick

A: Aufgabenstellung  
Mission Statement  
Kontextabgrenzung

B: Einfluss  
Rahmenbedingungen  
Top-Qualitätsziele

C: Lösungsstrategie  
Informelles Überblicksbild  
Entscheidende Lösungsansätze

D: Eintauchen in die Corona-Warn-App  
Zerlegung auf oberster Ebene  
Ausschnitt Technologie-Stack

E: Bewertung & Ausblick  
Ausgewählte Kompromisse  
Nächste Schritte für die CWA  
Weitere Informationen

→ <https://www.embarc.de/architektur-ueberblicke/#cwa>

#### Ausschnitt Technologie-Stack

Die Lösung verwendet diverse Programmiersprachen, Bibliotheken, Frameworks und Middleware.

Qualität insgesamt: 206.560 Lines of Code (100%)  
(April 2021, inkl. Tests)

Swift: 40,1%

Java: 20,4%

Kotlin: 39,5%

Client (Native App)

#### Server (Backend)

- Services programmiert in Java mit Spring Boot, Spring Cloud, Spring Data
- weitere Open Source Bibliotheken (u.a. Lombok, Guava, Libphonenumber, Micrometer, ...)
- Kommunikation mit REST/OpenAPI und protobuf
- Persistenz mit PostgreSQL

embarc Software Consulting GmbH  
Hamburg // Wien  
info@embarc.de  
www.embarc.de

# Vielen Dank.

Ich freue mich auf Eure Fragen!



**Falk Sippach**



fs@embarc.de



@sipsack



→ [xing.to/fsi](https://www.xing.to/fsi)

